

# Exhibit 202, part 2

## *Section 3 - Law Enforcement Cases*

This section of *The SAR Activity Review* affords law enforcement agencies the opportunity to summarize investigations where Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs) and other BSA information played an important role in the successful investigation and prosecution of criminal activity. This issue contains new case examples from federal, state and local law enforcement agencies. Additional law enforcement cases can be found on the FinCEN website, [www.fincen.gov](http://www.fincen.gov), under the link to [Investigations Assisted by BSA Data](#). This site is updated periodically with new cases of interest, which are listed by the type of form used in the investigation, type of industry involved and type of violation committed.

In many cases, SAR confidentiality requirements preclude FinCEN from associating the name of all law enforcement agencies and entities that utilized SAR information for specific cases highlighted in *The SAR Activity Review*. FinCEN appreciates the help and support of the following agencies and entities that contributed to the cases in this issue: The United States Attorney for the Eastern District of California, ICE, DEA, FBI, IRS, ATF, USPI, and the Connecticut State Police. Contributing editors: Shawn Braszo, Jennifer White, James Emery, and Jack Cunniff.

In this edition of *The SAR Activity Review*, we take a special look at fraud cases. We review several examples where SARs were used in or triggered investigations centering on the securities industry, traditional Ponzi schemes, and mortgage fraud.

Suspicious Activity Reports help law enforcement agencies investigate fraud cases and prosecute perpetrators in many ways, ranging from focusing complex, time-consuming investigations to paving the way for victims to obtain restitution. Often fraud cases are initiated on the basis of a SAR filing from a financial institution that noticed suspect transactions. In such cases, neither the victims nor law enforcement agencies may have been aware of the criminal activity. Once filed, these SARs are subsequently read by both SAR review teams and individual investigatory agencies, and with the SAR in their possession law enforcement can assess the size and scope of the fraud and investigate the crime, leading to prosecution of the defendants and possible restitution for the victims. Even when a case is not initiated from a SAR, the existence of such a report can provide invaluable leads to investigators.

*Financial Crimes Enforcement Network***Cases Involving the Securities Industry**

Immigration and Customs Enforcement (ICE) investigated two cases from the securities industry initiated from SARs that had wide impact and claimed many victims. In the first case, the perpetrators set up a boiler-room operation in the United States, but targeted victims in another country. An alert depository institution noted that account activity did not match the firm's stated business activity. In the second case, a securities broker notified U.S. Customs of suspect activity in a filing that originated before that industry had a regulatory requirement to file SARs.

***Guilty Pleas in International Hedge Fund Fraud Case Initiated from SARs***

An investigation into hedge fund fraud that was initiated from a SAR resulted in guilty pleas, forfeiture, and in the case of the ringleader, a lengthy prison sentence. The prosecution began several years ago when a federal grand jury charged four men in connection with the fraud. All of the victims were non-U.S. residents, and the international investigation utilized FinCEN's 314(a) information sharing process as well as exchanges of information through the Egmont Group of financial intelligence units.<sup>32</sup>

The leader of the scheme, a foreign national, entered the United States on an E-2 Treaty Investor Visa<sup>33</sup> and purported to be operating hedge funds and financial advisement firms which catered to wealthy citizens outside of the United States.

The leader had previously engaged in financial fraud in his home country and received a civil admonition in a non-U.S. court more than ten years ago. In addition to the civil admonition, the defendant received probation and was banned from operating any financial businesses in his home country. Around this time, the defendant came to the United States and started boiler room operations for the fraudulent hedge fund.

---

32. The Egmont Group of financial intelligence units (FIUs) is an international network designed to improve interaction among FIUs in the areas of communications, information sharing, and training coordination. The goal of the Egmont Group is to provide a forum for FIUs around the world to improve support to their respective governments in the fight against money laundering, terrorist financing and other financial crimes.

33. As a treaty investor, the Immigration & Nationality Act provides non-immigrant visa status for a national of a country with which the US maintains a treaty of commerce, who is coming to the US to carry on substantial trade or, to develop and direct the operations of an enterprise in which the individual has invested; or is in the process of investing a substantial amount of capital.

*Financial Crimes Enforcement Network*

The lead defendant in the fraud utilized his purported hedge fund consulting agencies to sponsor individuals who spoke his native language and were seeking work in the United States. The defendant applied for immigration status for his workers and utilized them as boiler-room operators. These individuals would contact wealthy citizens in the target country through a cold-calling technique and entice them to purportedly purchase stocks in the U.S. market. The operatives used data mining software to collect information from public sources, including individuals' and businesses' names, addresses and phone numbers. The data collected was then entered into a spreadsheet and used to make calls to potential investors.

Once investment funds were received via wire, the funds were transferred among several accounts controlled by the defendant and his co-conspirators. The funds were ultimately spent on personal and business expenses in furtherance of the fraud. Very few stocks were actually purchased with the funds. The defendant instructed his workers on how to use deceptive measures and lies to extract more money from unsuspecting investors. Investors who attempted to cash out their investments were instead persuaded to wire additional funds to meet fictitious withdrawal thresholds and subsequently lost even more money. The total estimated loss was approximately \$21 million from over 800 foreign investors.

When investigators interviewed the boiler room operators, the employees revealed that they were not aware of the fraud being perpetrated by the lead defendant. In fact, the defendant held fake board meetings with "board members" in which he also included the boiler room operators. During these meetings, the defendant discussed the stocks the business had invested in and the number of shares held in certain companies.

Two years prior to the indictment, a financial institution filed a SAR on the business and its president (the lead defendant) for a number of suspect activities. According to the SAR, the company's business was solely purported to be an advisor to hedge funds with all income limited to fees from those hedge funds. However, the bank noticed deposits originating from individuals in the target country. In addition, the principals of the company wired funds to companies controlled by the defendant. Finally, the SAR noted that foreign bank regulators had previously closed businesses related to the defendant for various violations, including improper licenses and illegal foreign exchange transactions.

*Financial Crimes Enforcement Network*

Soon after the financial institution filed the SAR, an analyst with the financial enforcement group of a law enforcement agency identified the filing during a routine review. The analyst conducted further research on the defendant and eventually referred the case to a task force for investigation. In addition to the SAR that identified the financial activity, a SAR filed by a broker-dealer highlighted more than \$1 million in questionable wire transfers. That SAR noted that a government office had identified 19 liens and judgments recorded against the defendant's business.

In the course of the investigation, more than \$400,000 in victims' funds were recovered and seized from bank accounts. Another \$100,000 was seized from brokerage accounts. Investigators identified accounts overseas, including European countries known for their private banking services to non-residents. The lead defendant received a prison sentence of more than 15 years and was ordered to forfeit more than \$20 million to be used for restitution to victims of the fraud.

### ***Securities Dealer Provides Details of High Yield Investment Program Scheme***

Six defendants pled guilty and received prison time for defrauding investors in a case that started when a securities firm noticed suspect transactions and reported the activity to law enforcement. The defendants created a bogus investment scheme, marketed it over the Internet, and defrauded nearly 200 investors from around the world of more than \$16 million.

The case began in 1998 when a task force received a suspicious activity report from a brokerage firm regarding five related accounts. The brokerage firm did not file a SAR with FinCEN, as broker/dealers did not have a regulatory obligation to file SARs at that time, but maintained a close relationship with law enforcement and instead handed a paper document to U.S. Customs. The paper document was subsequently lost in the September 11 terrorist attacks on the World Trade Center in New York City.

An analysis of the accounts and documents in the possession of the brokerage firm, though, indicated that the subject business account was acting as a collection account for millions of dollars that were being sent from locations inside and outside the United States. Once received into this account, the funds were either journal transferred to one of the related accounts or transferred out of the United States. The



*Financial Crimes Enforcement Network*

funds that were journal transferred to other brokerage firm accounts were transferred out of these accounts to bank accounts in the United States and abroad or used to pay for personal expenses of those involved in the fraud scheme.

The defendants' convictions resulted from their development and orchestration of an elaborate scheme to defraud investors. More than ten years ago, the two primary defendants in the scheme began holding themselves out to investors as promoters of a high-yield investment program that promised massive returns within a short period of time. The defendants created a series of fictitious European banks from which investors were to "lease" funds to invest, normally for a leasing fee of about \$35,000. Payment of this fee would purportedly release \$1 million, which the defendants claimed would then be placed in the high-yield trading program. In reality, no funds were released and the investment programs were nonexistent.

The defendants pocketed the leasing fees and eventually defrauded victims out of approximately \$17 million. As the number of victims increased, and the scheme became more complicated, the defendants recruited subordinates to help maintain the illusion that brokers were recommending the investment programs and that the banks were actual financial institutions. Three of these subordinates pled guilty in the case.

In addition to the plea allocutions, the government's case at trial rested on the voluminous documentary evidence recovered during searches of the defendants' residences, including forged documents used to assure the victims that their "leased" funds were available for investment. Several victims testified, as did foreign and American banking officials who established that the banks created by the defendants were fictitious. Both lead defendants were convicted on all counts.

At the time the business accounts with the broker-dealer were discovered, the total amount collected in the account was approximately \$14 million. An additional \$2 million was located in a European country. Investigators eventually seized assets worth in excess of \$10 million which have been used to make restitution to defrauded victims. The architects of the scheme were convicted in a jury trial of conspiracy, wire fraud, money laundering, and interstate transportation of stolen property; one received a prison sentence of more than 16 years and the other received a sentence of more than 11 years.

*Financial Crimes Enforcement Network***Traditional Ponzi Schemes**

While some large-scale Ponzi schemes have made headlines in the past few months, similar schemes have been defrauding innocent victims for years. BSA records, particularly SARs, have become an important tool for fighting Ponzi schemes. In this edition, we include three examples of how SARs contributed to the investigations of Ponzi schemes. In the first case, a SAR was the launching point for an investigation. In the next two similar but separate cases, subjects previously apprehended for fraud attempted to pay court-ordered restitution (and steal more money) by creating even more sophisticated frauds. These last two examples highlight the synergy of know-your-customers policies and suspicious reporting. In particular, these cases exemplify how well-researched and well-written SARs ultimately benefit consumers and taxpayers.

***SAR Jump-Starts Investigation into Natural Resources Ponzi Scheme***

A purported entrepreneur convinced scores of individuals to invest in ventures and businesses supposedly related to the extraction of natural resources that were, in reality, part of a sophisticated Ponzi scheme. The defendant followed a familiar pattern evident in such schemes: paying earlier investors with funds from new investors as well as keeping a substantial amount for himself. When victims first complained about the defendant, law enforcement had little information on him and few leads. Around the same time that victims were contacting law enforcement, a financial institution also filed a SAR on a suspect transaction. When victims made subsequent complaints, agents located the SAR and launched a full-scale investigation that resulted in an arrest within a few months.

The scheme ran for about 5 to 6 years, with the defendant generally promising to double investors' money within one year. In all, he raised about \$10 million from about 100 investors. The defendant memorialized the investors' loans in a series of promissory notes and security agreements, in which he pledged as collateral the various natural resources to be extracted from property that he leased. He flagrantly overstated the value of the collateral as he tried to induce prospective investors. Contrary to his promises that he would use the funds for various business-related purposes, he in fact used a substantial portion of the money he raised to make partial payments to earlier investors and to support a lavish personal lifestyle.

*Financial Crimes Enforcement Network*

The defendant was arrested and charged in the scheme and while on pre-trial release improperly tried to solicit more money from investors. All together, three banks where the defendant held accounts filed SARs on suspicious transactions. Many of the transactions listed in the SARs directly led to the charges included in the complaint and indictment. The SARs describe how the defendant frequently asked his investors to write checks to third parties, claiming that they were only to show new investors that the ventures had financial backing. However, the defendant frequently cashed or deposited these checks.

A federal judge sentenced the defendant to more than 10 years in prison following his guilty plea to counts of mail fraud, wire fraud, bank fraud, and money laundering. The presiding judge ordered that he serve five years of supervised release following completion of his prison term and pay restitution totaling almost \$10 million.

***Bank SARs Lead to Discovery of Predatory Certificate of Deposit Fraud Scheme***

In order to satisfy fines and restitution ordered as a result of an earlier scheme, two defendants began a new multi-state advertising campaign scheme to attract buyers (mostly elderly) of non-existent certificates of deposits.

As part of the scheme, one of defendants rented office space in one state and hired workers to handle investor inquiries. He also established a mail drop in a distant city to receive investor payments. The mail drop in that city had instructions to forward all mail to a second mail drop in yet another state. Investors mailing payments to that mail drop were told to make the checks payable to another company that was actually a shell company. To convert the investor payments into personal cash, the second defendant opened a series of shell bank accounts. After reviewing transactions related to the accounts, the bank filed a SAR and notified law enforcement.

The bank SAR that initiated the case noted that one of the defendants opened accounts for several businesses that ultimately turned out to be fronts for the fraud scheme. The bank noticed that checks made out to one business were deposited into the account of another business. In addition, the bank believed the transactions in the account were indicative of fraud because there appeared to be no discernable legitimate business activity, only small monthly payments to individuals that appeared to be interest payments.



*Financial Crimes Enforcement Network*

The SAR narrative described critical elements of the crime in detail. The bank noted that the age of the investors ranged from approximately 60 to 90 years of age, and the checks had notations on the memo lines consistent with the purchase of Certificates of Deposit. The withdrawals from the account were in the form of checks made out to cash in amounts ranging from \$4,000 to \$9,500. And, as indicated, the only activity in one account was small monthly checks to individuals.

Bank staff asked numerous questions of one of the defendants, and his responses reinforced their fears that he operated a predatory fraud scheme aimed at senior citizens. The bank froze one of the accounts with a balance of almost \$400,000. The defendant responded with only a cursory protest and said he would contact his lawyers. The bank explained the circumstances to the defendant's lawyer but the defendant took no further action in the matter.

Law enforcement and prosecutors noted that the SAR proved instrumental in ending the scheme and the funds in the frozen account provided restitution for some victims. The two defendants were sentenced for their roles in the scheme. One received a 30-year prison sentence in exchange for a guilty plea for his role in the two fraud schemes. In addition, he was ordered to pay almost \$5 million in restitution. The severity of the sentence, unusual for white-collar crime with a plea agreement, stemmed from the defendant's role as leader in both schemes as well as his refusal to account for the stolen funds. His co-defendant also pled guilty and received a sentence of more than 7 years.

***Bogus Life Insurance Investment Vehicles Identified through SAR Filing***

The defendants in this case first settled a civil suit with the government concerning the sale of \$7 million worth of fraudulent "prime-bank" note investments to investors nationwide. In the scheme, investigators found that less than half the money was used to pay fictitious investment returns to existing investors. The rest was used by the perpetrators of the fraud for personal expenditures.

The defendants then orchestrated a Ponzi scheme in which they solicited more than \$60 million from dozens of investors, according to court documents. The pair told investors that their money would be used to purchase pools of life insurance policies on behalf of an organization. In return, a small portion of the death benefit would go to the family of the insured, but the majority of the money would be paid back to the defendants' company. Investors were promised they would receive a high annual return and were told their "risk-free" investments would eventually yield a five-to-one return.

*Financial Crimes Enforcement Network*

Prosecutors charged that only a fraction of the funds were used to purchase two pools of life insurance policies, and that approximately \$60 million was used by the defendants to further their lavish lifestyles, including the purchase of houses, cars, boats, and jewelry. One defendant also transferred approximately \$10 million in investor funds to an unrelated business venture.

The investigation into the Ponzi scheme started with a SAR filed by a depository institution. The SAR narrative described how, during routine due diligence in the wake of the press reports concerning the original government action on the prime bank guarantees, the filing institution realized that the defendants had a number of accounts at the institution. One account had more than \$15 million in unusual transactions credited to it in a three-month period.

An agent investigating the case noted that the SAR proved “absolutely crucial” to the success of the case. Because of the filing, law enforcement was able to unravel the scheme quickly. In less than a year, and from a reported \$1 million in losses, agents uncovered more than \$60 million in fraudulent transactions resulting in the indictment and arrests of the subjects. Moreover, additional BSA filings on the subjects helped agents find assets that were seized for restitution.

## **Mortgage Fraud Cases**

FinCEN has reported on the increase in the number of SARs that cite mortgage fraud as a potential violation.<sup>34</sup> Law enforcement uses these SARs to investigate and prosecute mortgage fraud cases, two of which are recounted here. In the first case, depository institutions filed SARs on both the defendant’s business and personal accounts. When the lead investigator identified these SARs, he established a close working relationship with the institutions which facilitated the flow of information necessary for a quick arrest of the subject. In the second case, the extra effort on the part of the depository institution in developing information on a defaulting mortgage holder helped identify a mortgage fraud ring.

---

34. See [Mortgage Loan Fraud Connections with Other Financial Crimes](#) and [Filing Trends in Mortgage Loan Fraud](#). Additional information on Mortgage Fraud is available on FinCEN’s website, [www.fincen.gov](http://www.fincen.gov).

*Financial Crimes Enforcement Network****Case for Mortgage Fraud Involving Straw Buyers Supported by SARs***

BSA records helped identify co-conspirators, accounts, and elements of a mortgage fraud scheme that may total as much as \$7 million dollars in losses. SAR filings described transactions related to the fraud in both personal and business accounts belonging to the defendant in the case, and CTRs filed by a bank and a money services business identified currency transactions that were consistent with fraudulent activity.

In a scheme that lasted for approximately three years, the defendant and his co-conspirators profited by selling residential real estate in the Mid-Atlantic area to individuals acting as straw buyers. The defendant and his co-conspirators, through a business the defendant established, helped the straw buyers obtain 100% mortgage financing to purchase the properties. To obtain the mortgage financing, the conspirators produced fraudulent loan applications that included materially false statements related to the buyers' employment, income, immigration status, and intent to occupy the properties as primary residences. The straw buyers frequently defaulted on these mortgages, causing losses to banks and commercial lenders in excess of \$2,500,000.

During the period that the fraud was being perpetrated, several banks filed SARs noting unusual patterns of activity. SARs filed on the defendant's business note that the applicants for the loans may have overstated employment and inflated salaries, lied about the use of the home as a primary residence, or provided other information that created discrepancies indicative of mortgage fraud. SARs filed on the defendant's personal accounts highlighted patterns of structured withdrawals as well as cashier's checks that were cashed in a manner consistent with fraudulent behavior.

Investigators who reviewed the SARs reached out to the respective banks for more information on the defendant and his co-conspirators. The banks continued to monitor the accounts closely, filed additional SARs, and simultaneously notified the lead investigator. A bank noted in one SAR that certain suspect transactions involving official checks did not appear to serve any logical business or personal reason. The bank also noted as unusual the receipt of wires and checks from title companies into a personal account by an individual who has a mortgage lending business.

A federal judge sentenced the defendant to more than five years in prison, followed by supervised release, and ordered him to pay several million dollars in restitution.

*Financial Crimes Enforcement Network****Proactive Suspicious Activity Report Review Leads to Guilty Pleas in “Cash Back” Mortgage Fraud Scheme***

In a case that started from a proactive review of Suspicious Activity Reports, a specialized mortgage fraud task force launched an investigation that led to charges against two individuals. Bank Secrecy Act records captured many of the scheme’s intricate details, including a SAR filed on one of the defendants who was described as being “very upset” when he learned that a CTR would be filed as a result of a series of transactions.

According to the assistant United States attorney who prosecuted the case, the indictment charged that over an 18 month period the defendants engaged in a scheme to defraud mortgage lenders in connection with residential real property purchases. The leader of the scheme recruited various individuals, including straw and nominal purchasers, to purchase more than a dozen real properties. In addition, the leader orchestrated the transactions and conspired with a mortgage broker to complete the fraud.

The indictment charged that the transactions involved fraudulent or false representations in obtaining 100% mortgage financing, including misstatements about the purchasers’ monthly income, intent to occupy the property, and existing liabilities. In addition, the indictment alleged that in each transaction the purchase price was above the true market price of the property. An amount approximately equal to the difference between the purchase price and the true market price was diverted as “cash back” at the close of each escrow into the bank account of an out-of-state corporation. As part of the scheme, the defendant caused these credits to be concealed from the mortgage lenders. The indictment charged that the defendant in fact exercised control over the out-of-state corporation bank account and used the fraudulently obtained funds for various purposes, including extensive cash withdrawals.

The case originated after a SAR review team identified a SAR filed on one of the straw buyers, an associate of the defendant. Because the SAR listed mortgage loan fraud as the suspected violation type, the team referred the SAR to a mortgage fraud task force. The SAR filer noted that the subject (the aforementioned straw buyer) apparently misrepresented information on a loan application for a mortgage that was in default. The co-conspirator and mortgage broker acted as the loan agent and broker of record on the loan. Through research, the filing institution found that the subject had purchased four additional properties for which each mortgage loan totaled at least \$490,000. All properties were closed by the same title company.

*Financial Crimes Enforcement Network*

Investigators identified several additional related SARs, including one with a lengthy narrative describing activity on 18 individuals and businesses associated with the scheme. Investigators included many of the details described in the SARs in a criminal complaint and as evidence in the indictment charging the defendant and co-conspirator. One SAR noted that a co-conspirator became irate when he learned that a CTR filing was required following a series of transactions.

The original criminal complaint described in detail the defendant's efforts to defraud lenders through straw buyers. While the defendant approached the buyers to invest in properties and open bank accounts, he actually controlled all aspects of the purchases and the accounts. Although the buyers provided the defendant with truthful personal information, the defendant made false representations on the loan applications in regard to income, employment, and intent to occupy the residences.

In late 2008, the leader of the mortgage fraud scheme pled guilty to mail fraud and structuring currency transactions at a financial institution to evade the reporting of the transactions. The total losses in the fraud exceeded \$2.5 million.

*Investigating agencies include Federal, State agencies and Local Police Departments.*



## ***Section 4 - Issues & Guidance***

**T**his section of *The SAR Activity Review* discusses current issues raised with regard to the preparation and filing of SARs. This section is intended to identify suspicious activity reporting-related issues and provide meaningful guidance to filers. In addition, it reflects the collective positions of the government agencies that require organizations to file SARs.

On March 3, 2009 FinCEN announced a [Notice of Proposed Rulemaking](#) on the Confidentiality of Suspicious Activity Reports. Also on March 3, FinCEN proposed [Interpretive Guidance](#) on the sharing of suspicious activity reports by securities broker-dealers, mutual funds, futures commission merchants and introducing brokers in commodities with affiliates that are also subject to SAR rules. The Notice of Proposed Rulemaking and the proposed Interpretive Guidance were posted to the Federal Register on March 3, and financial institutions are encouraged to provide written comments, which may be submitted to FinCEN through June 8, 2009.

### **Identifying and Reporting Suspicious Transactions for Introducing and Clearing Broker-Dealers**

*By FinCEN Office of Regulatory Policy*

Since the passage of the USA PATRIOT Act and the promulgation of enhanced requirements for the securities industry, there has been significant attention focused on the anti-money laundering requirements of introducing and clearing broker-dealers.

*Financial Crimes Enforcement Network*

In the securities industry, it is common for “introducing” firms to enter into arrangements with “clearing” firms that establish the responsibility of each firm with respect to functions required to be performed, from opening the account to sending confirmations and statements to the customer. These clearing agreements, which are done pursuant to the rules of a self-regulatory organization, most typically allocate to the introducing firm the responsibilities for opening and approving accounts and taking and receiving orders. The clearing firm most commonly takes on the responsibilities for extending credit, executing and settling transactions, safeguarding funds and securities, and issuing confirmations and statements.

With respect to AML compliance, introducing and clearing brokers generally have independent responsibilities. In March 2008, FinCEN issued a no-action position with respect to the requirements under the Customer Identification Program Rule. FinCEN has also addressed obligations of clearing firms with respect to the Correspondent Account and Private Banking Rules under section 312.<sup>35</sup> In addition, the Financial Industry Regulatory Authority (FINRA) has issued certain information since the passage of the USA PATRIOT Act addressing the SAR reporting obligations of introducing and clearing firms.<sup>36</sup>

Key Points for Suspicious Activity Reporting

1. The obligation to identify and report a suspicious transaction rests with each broker-dealer involved in a transaction.
  - Both introducing and clearing brokers have independent obligations to monitor account activity for suspicious transactions.
  - Introducing and clearing firms may coordinate their activities to detect suspicious activity to allow each firm to meet its obligations to comply with its SAR requirements.
    - Introducing firms may be in better position to monitor activity in connection with opening the account and communicating directly with the customer. Clearing firms may be in a better position to monitor customer transaction activity, including for example trading, wire transfers and cash movements into and out of the account.

---

35. See *Application of the Regulations Requiring Special Due Diligence programs for Certain Foreign Accounts to the Securities and Futures Industries*, FIN-2006-G009 (May 10, 2006).

36. See NASD Notice to Members 02-21 (April 2002) and FINRA Small Firm Template (Last updated January 23, 2004), available at <http://www.finra.org/Industry/Issues/AML/P006340>.

*Financial Crimes Enforcement Network*

- In some situations, clearing firms may be able to develop tools or enhance existing tools which might assist introducing brokers in analyzing the transactional activity of its customer.
2. Introducing brokers and clearing firms may develop effective communication procedures that permit coordination when questionable activity or potential indications of suspicious activity are detected by either firm.
- Introducing and clearing firms involved in a transaction may share information about that particular suspicious transaction for purposes of determining which firm will file a SAR.
  - Introducing and clearing firms involved in a transaction may opt to file a joint SAR-SF, but the report must include all relevant facts covering the transaction or pattern of transactions. The purpose of this provision is to allow two broker-dealers that have participated in the same transaction or pattern of transactions to file only one SAR. However, each firm involved in the joint filing must maintain supporting documentation on the SAR filing.
  - Firms should remember that the disclosure limitations found in 31 U.S.C. 5318(g)(2) on dissemination of the SAR, and disclosure of the fact of its filing, apply equally to both broker-dealers that are jointly filing a SAR.
  - The introducing broker and clearing broker may have separate criteria for evaluating the transactions and may make different determinations as to whether a suspicious activity report is required to be filed. In cases where a SAR is not jointly filed, the filing institution may not disclose to the other broker that a SAR has been filed.
  - Introducing and clearing firms may file notices under the Section 314(b) safe harbor to share information that may involve possible terrorist or money laundering activities, as permitted for all financial institutions complying with the 314(b) rule. Such information sharing may allow firms to identify and report activities that may involve terrorist acts or money laundering and to determine whether to open or maintain an account or engage in a transaction. Firms should note, however, that although information shared under the 314(b) program enjoys the benefit of safe harbor protection, the 314(b) safe harbor does not cover the disclosure of a SAR or information indicating that a SAR has been filed. Firms must, therefore, abide by the rules governing SAR confidentiality.

*Financial Crimes Enforcement Network*

Broker-dealers that are either introducing or clearing firms should remember that each has independent responsibilities to identify and report suspicious activity. While introducing and clearing firms may allocate certain monitoring functions in a fully disclosed clearing agreement,<sup>37</sup> this does not alter their separate and distinct obligations under the SAR rule. For example, when a clearing firm is not allocated the responsibility of monitoring customer accounts according to the terms of a fully disclosed clearing agreement, it nonetheless is obligated to establish policies, procedures, and controls that are reasonably designed to detect and report suspicious activity that is attempted or conducted by, at, or through it, including activity that is introduced to it by another firm.<sup>38</sup> Moreover, firms may develop effective communication procedures when potential indications of suspicious activity are detected to ensure that each firm is able to satisfy its suspicious activity reporting requirements.

## **SAR Form Completion When Reporting Identity Theft**

*By FinCEN Office of Regulatory Policy*

Identity theft occurs in many forms and can include additional crimes of false statement, computer intrusion, credit or debit card fraud, mortgage loan fraud, or wire transfer fraud. As a means of better identifying and tracking known or suspected criminal violations of identity theft, a financial institution should report identity theft and any additional suspicious activities involved on a SAR. In situations involving multiple violations of law, reporting identity theft in conjunction with additional suspicious activities can be of significant assistance to law enforcement. This serves to notify law enforcement of the nature of the activity and may be valuable to law enforcement personnel in seeking a greater awareness of an entire pattern of activity.

---

37. NYSE Rule 382 and NASD Rule 3230 (permitting clearing and introducing firms to allocate regulatory and operational functions between them, including the responsibility for opening, approving and monitoring accounts; extending credit; maintaining books and records; receiving and delivering funds and securities; safeguarding customers funds and securities; issuing trade confirmations and account statements; and accepting orders and executing transactions).

38. See 31 C.F.R § 103.19(a)(2).



*Financial Crimes Enforcement Network*

It is important that the SAR narrative contain a full picture of the suspicious activity involved. The narrative should be a chronological and complete account of the possible violation of law. For example:

- A suspect accesses the victim's investment account via the internet using the victim's name and account information and places trades for all of the securities in the account. The suspect then attempts to wire the proceeds to a bank account in a foreign country. The broker-dealer becomes aware of the identity theft after contacting the victim to verify the unusual account activity and the unusual destination of the wire transfer.
- A suspect establishes an investment account with a broker-dealer via the internet using the victim's personal information and attempts to wire funds from the victim's bank account. The account activity appears legitimate. The broker-dealer becomes aware of the identity theft only when informed by the victim's bank that the transfer of funds is unauthorized.

The SAR narrative should include information about the suspect (if available), how the account was accessed, if the attempt involved an online virus (e.g., a trojan or spyware) and what instruments or mechanisms were used in the transaction(s). The narrative should also include the accounts involved, the date and period of time the suspicious activity took place, whether the attempt appears duplicative and frequently occurred in different customer accounts, the place the activity occurred, whether a foreign jurisdiction was involved, whether another financial institution was involved, how the identity theft was detected, and why the activity is suspicious.

Further, it is important to note that all filers should ensure that they have provided as much detail as possible in the narrative regarding the suspect and activities involved in the identity theft. Unless the victim is suspected to have contributed to the identity theft scheme, the victim is not a suspect. If suspect information is unknown or unavailable, any partial or incomplete identifying information should be included. For example, a suspect through a trojan online-virus obtains personal information of the victim, contacts the victim's bank by phone and submits a notice of a change in address and requests for a new or additional debit/credit card. The filer when completing the narrative may be able to provide the suspect's address and phone number used to contact the bank.

Alternatively, the suspect information may be unknown or unavailable. For example, a suspect using the victim's personal information may attempt a transaction, such as a funds transfer at the victim's bank, but when asked for identification cannot provide



*Financial Crimes Enforcement Network*

authenticating information and terminates the transaction. In these instances, the financial institution should include whatever identifying information is available (email address, description, etc.) in the narrative.

## **Global Resolution of Potential Enforcement Actions**

*By FinCEN Office of Enforcement*

A broker-dealer, mutual fund, or futures commission merchant in violation of requirements to implement adequate measures reasonably designed to ensure compliance with the Bank Secrecy Act (BSA), including detection and reporting of suspicious activity indicative of money laundering, terrorist financing, or other financial crimes, may be subject to enforcement actions by multiple government agencies.<sup>39</sup> FinCEN may assess civil money penalties against a broker-dealer, mutual fund, or futures commission merchant for violating the BSA.<sup>40</sup> In addition, the U.S. Securities and Exchange Commission (SEC), Financial Industry Regulatory Authority (FINRA), or U.S. Commodity Futures Trading Commission (CFTC) may also take enforcement action, under their respective jurisdictions,<sup>41</sup> for violations of counter-money laundering requirements similar to, but separate from, the BSA.

When charged with conduct violating the BSA and other counter-money laundering requirements, a broker-dealer, mutual fund, or futures commission merchant should consider seeking global resolution of all potentially related enforcement matters. While the SEC, FINRA, CFTC, and FinCEN must operate under their distinct jurisdictional authorities, we strive, whenever possible, to proceed jointly and concurrently on enforcement matters. Global proceedings advance disposition of BSA enforcement matters in the context of other related matters, and avoid potential for multiple actions against a financial institution at different times for similar or related conduct. In addition, global enforcement actions advance consistent and uniform enforcement of the BSA and other counter-money laundering requirements by all stakeholder government and self regulatory organizations.

39. See U.S. Government Accountability Office, Bank Secrecy Act, Federal Agencies Should Take Action to Further Improve Coordination and Information-Sharing. GAO-09-227 (February 2009).

40. 31 U.S.C. § 5321 and 31 C.F.R. § 103.57.

41. See e.g., Securities Exchange Act of 1934 sections 21B and 21C.

## ***Section 5 - Industry Forum***

In each issue of *The SAR Activity Review*, representatives from the financial services industry offer insights into some aspect of compliance management or fraud prevention that present their view of how they implement the BSA within their institutions. The *Industry Forum* section provides an opportunity for the industry to share its views. The information provided may not represent the official position of the U.S. Government.

### **Ensuring Effective Broker-Dealer SAR Programs**

*By Alan E. Sorcher and R. Stephen Ganis<sup>42</sup>*

Notwithstanding all of the USA PATRIOT Act rules that broker-dealers are required to comply with, suspicious activity monitoring and reporting remains at the heart of a firm's compliance program. While the SAR rule is far from new, firms must ensure that their program is kept current and relevant. Failure to do so can put a firm at risk of missing detectable suspicious activity and, potentially, violating the BSA. The spate of allegations stemming from the financial crisis about illegal activity in the securities markets, moreover, presents an opportunity for broker-dealers to review the scope and methodology of their suspicious activity detection and reporting practices.

---

42. At the time of writing this article, Alan E. Sorcher was General Counsel of the Bankers Association for Finance and Trade. R. Stephen Ganis is Of Counsel at the law firm of Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. Both authors have served on the U.S. Department of the Treasury Bank Secrecy Act Advisory Group and various sub-committees thereof.

*Financial Crimes Enforcement Network***Background**

One of the biggest challenges of the SAR rule is the wide net that it requires firms to cast. The rule, in general, requires the reporting to FinCEN of any “suspicious transaction relevant to a possible violation of law or regulation” of at least \$5,000 in funds or other assets that is conducted or attempted by, at, or through the broker-dealer. Broker-dealers should remember that securities law violations are covered. The rule allows firms to follow a risk-based approach in monitoring for suspicious activity. Firms are expected to “evaluate customer activity and relationships for money laundering risks and design a suspicious transaction monitoring program that is appropriate . . . in light of such risks.” Thus, a firm can fashion a SAR program that makes sense for its business so long as it appropriately addresses the suspicious activity risks inherent in that business.

A difficult aspect of risk-based SAR programs is that the risks confronting broker-dealers are constantly changing. The events of the past year have demonstrated that things are often not what they seem and firms should pay careful attention to the widening range of transactions that might be deemed to pose suspicious activity risks. Types of transactions by, at or through broker-dealers that were thought to pose little or no risk of suspicious activity a year ago may, when analyzed in light of intervening events, be found to pose increased risks today. With that in mind, here are some basic points to help keep your SAR program up to speed.

**Addressing Current Events and Emerging Trends*****Financial Crisis***

The current financial crisis, which resulted in two significant impacts on broker-dealer suspicious activity detection and reporting practices, has shown that financial institutions must try to be prepared for the unpredictable.

First, the crisis has changed the nature, size and volume of transactions that need to be monitored for potential suspicious activity. Systems and processes using customer profiles and rule parameters based on pre-existing notions of “normal” transaction sizes and volumes may need to be adjusted to reflect current market realities. Indeed, enormous movements and volatility in the markets over the past year have made it more difficult for firms to use stock price or volume swings to help identify suspicious activity.

*Financial Crimes Enforcement Network*

Second, the crisis has revealed suspicious activity risks that might not have been apparent before. Firms should therefore pay close attention to current events and emerging risks and, when appropriate, incorporate them into their SAR program. Recent cases demonstrate vulnerabilities to suspicious activity in transactions with or on behalf of even those customers with top reputations. Just as the crisis has highlighted the potential vulnerability of the lending industry to mortgage fraud, it has similarly highlighted the vulnerability of the brokerage industry to securities fraud and manipulation. For example, federal regulators have alleged widespread manipulative short sales and credit default swaps trading by certain kinds of institutional customers of broker-dealers. Regulators in other countries have responded to similar allegations in foreign markets by issuing guidance clarifying that potentially manipulative short sales are subject to mandatory suspicious transaction reporting by market intermediaries. The crisis has also highlighted risks associated with certain custody arrangements, for example risks arising when institutional customers act as their own custodian without appropriate safeguards. Therefore, broker-dealers may wish to evaluate the extent to which recent allegations and revelations in the current financial crisis might impact the risk assessment underlying their suspicious activity detection practices.

**Cyber Crime**

Broker-dealer SAR programs should appropriately address the rapidly escalating threats posed by cyber crime. The potential harm to financial institutions in this area is significant. Particularly relevant to broker-dealers are several cases the SEC has brought involving online brokerage accounts, in particular with fraud relating to account compromise. The schemes typically combine electronic intrusion into online brokerage accounts with traditional market manipulation. A typical manipulative scheme involves traders hacking into investors' online accounts, selling the investor's securities positions, and using the proceeds to purchase shares of stocks subject to the scheme in a way that artificially inflates their price. Another common scheme involves theft from compromised accounts through electronic funds transfers. While these cases may be more relevant to firms that permit customers to transact online, they should not be ignored by the rest of the industry. Cyber crime continues to grow and firms should be on alert for red flags that may signal that something is amiss.

*Financial Crimes Enforcement Network****Trade-Based Money Laundering***

While historically more of an issue for banks, broker-dealers increasingly need awareness about trade-based money laundering. Because of the increasing focus by banks and their regulators on the trade-based money laundering threats arising in traditional letter of credit financing, there is a danger that laundering through trade might migrate to non-banking financial institutions. Thus, broker-dealers processing frequent or large cross-border payments, especially wire transfers, should consider evaluating their vulnerability, if any, to trade-based money laundering red flags. Trade-based money laundering can occur through under- or over-invoicing or routing several invoices through various financial institutions, leading to multiple payments for the same goods. There have also been cases where the quantity, quality and type of goods and services have been misrepresented, or where the shipping and customs documents differ from what is actually shipped. As participants in illicit trade finance grow more sophisticated about evading the intensifying scrutiny, it has become increasingly difficult to assess the genuineness of international trade transactions. Thus, broker-dealers with a large international presence may, depending on their business model, need to review whether necessary measures addressing emerging trade-based money laundering threats, if any, are necessary.

***Reported Suspicious Activity***

A SAR program should address current suspicious activity events and emerging trends not only within the broader securities markets generally, but also within the firm itself. Much can be gained from firms taking full advantage of actual suspicious activity they have reported, evaluating select SAR filings for broader trends and reviewing enforcement actions. All of these may be an excellent source of training and red flags that some firms may not be utilizing to the extent possible. Firms may need to make changes in their systems in response to reported suspicious activity. Names mentioned on SARs may aid in monitoring and customer due diligence. In addition, applying resources to evaluating SAR filings for broader trends may have significant benefit. Firms may be able to identify similar schemes, common locales or names, or possible red flags. Last, broker-dealers should follow enforcement actions involving securities fraud or manipulation occurring through brokerage accounts and relationships, and BSA and criminal money laundering violations more generally. These can reveal vulnerabilities that need to be addressed and areas of concern for the regulators.



*Financial Crimes Enforcement Network***Identification and Analysis of Transaction Types**

One challenge associated with implementing an effective SAR program is identifying all the types of transactions “by, at or through” a financial institution that are potentially subject to SAR filing requirements. This challenge is particularly pronounced for broker-dealers because typically more kinds of transactions occur in a brokerage account than in, for example, a demand deposit account. In addition to the full range of cash management and payment transactions associated with most bank accounts, brokerage accounts often permit a wide range of securities investment and trading activities. Most securities transactions are covered by the definition of “transaction” applicable to a SAR filing and include a “purchase or sale of any stock, bond, ... or other ... security ... or any other payment, transfer or delivery by, through or to a financial institution, by whatever means effected.” This definition is broad enough to capture not just monetary transactions (e.g., wire transfers, check deposits and disbursements, bill payments, automated clearinghouse and other electronic funds transfers, and other “cash” transactions) but also securities transactions, including purchases, sales, certificate of deposits, full and partial automated customer account transfers, free deliveries and receipts, external withdrawal by transfers, and internal journal entry transfers. Recent FINRA enforcement actions demonstrate compliance risks presented when a broker-dealer’s suspicious activity monitoring and detection efforts do not focus sufficiently on those securities transactions that are not accompanied by monetary transactions.

It may be a worthwhile exercise for a broker-dealer to go periodically through each type of transaction processed in the accounts it introduces or carries, whichever applies, to confirm the extent to which:

- suspicious activity detection systems or processes in place address the risks posed by the transaction type in each relevant business line; and
- any additional suspicious activity detection measures that may be necessary.

Because the universe of transaction types offered or processed by broker-dealers changes frequently, a transaction-by-transaction analysis of suspicious activity detection measures and gaps may need to be updated over time. In particular, business and operational changes such as automation of manual processes, migration of transaction processing from one systems environment to another, and roll out of new products or services may change the universe of transactions subject to SAR filing requirements that occur “by, at or through” a particular broker-dealer.

*Financial Crimes Enforcement Network***Identification of Detection Points**

Another ongoing practical challenge for a broker-dealer in maintaining an effective SAR program is ensuring that the anti-money laundering officer or unit coordinates sufficiently with all points in its organizational structure that might detect or otherwise become aware of potential suspicious activity that could require a SAR filing. This means that potential suspicious activity may need to be escalated not just by employees who handle SAR compliance but also by other departments. In this connection, broker-dealers may wish to review individuals or teams that handle the following types of matters to validate that they are, where necessary, incorporated adequately into escalation workflows:

- identity theft, account compromise, true name fraud, and check fraud;
- insider trading, market manipulation and other securities fraud;
- matches between customer accounts and information sharing requests sent to the broker-dealer through FinCEN pursuant to Section 314(a) of the USA PATRIOT Act;
- law enforcement and regulatory subpoenas;
- customer tax issues;
- customer due diligence (regulatory/disciplinary history, etc.);
- credit reviews of customer relationships and trading activity;
- operations (branch, treasury/cashiering, purchase/sale, foreign securities, restricted securities, physical deposits, and safekeeping);
- interactions with other firms concerning customer account activity; and
- employee financial crime or prohibited trading.

**Conclusion**

Maintaining an effective SAR monitoring and reporting program poses challenges for firms, and the recent market disruptions have increased those challenges. However, the compliance and reputation benefits for firms being able to root out potential wrongdoing at an early stage are quite apparent – and can be accomplished through a rigorous and flexible surveillance program that reflects emerging suspicious activity threats in an unusually dynamic capital markets environment.

## Financial Crimes Enforcement Network



## Section 6 - Feedback Form

### Financial Crimes Enforcement Network

U.S. Department of the Treasury

Your feedback is important and will assist us in planning future issues of *The SAR Activity Review*. Please take the time to complete this form. The form can be faxed to FinCEN at (202) 354-6411 or accessed and completed online at <http://www.fincen.gov/feedback/fb.sar.artti.php>. Questions regarding *The SAR Activity Review* can be submitted to [sar.review@fincen.gov](mailto:sar.review@fincen.gov). For all other questions, please contact our Regulatory Helpline at 1-800-949-2732. **Please do not submit questions regarding suspicious activity reports to the SAR Activity Review mailbox.**

A. Please identify your type of financial institution.

**Depository Institution:**

- ☐ Bank or Bank Holding Company  
☐ Savings Association  
☐ Credit Union  
☐ Foreign Bank with U.S. Branches or Agencies

**Securities and Futures Industry:**

- ☐ Securities Broker/Dealer  
☐ Futures Commission Merchant  
☐ Introducing Broker in Commodities  
☐ Mutual Fund

**Money Services Business:**

- ☐ Money Transmitter  
☐ Money Order Company or Agent  
☐ Traveler's Check Company or Agent  
☐ Currency Dealer or Exchanger  
☐ U.S. Postal Service  
☐ Stored Value

**Casino or Card Club:**

- ☐ Casino located in Nevada  
☐ Casino located outside of Nevada  
☐ Card Club

☐ Dealers in Precious Metals, Precious Stones, or Jewels

☐ Insurance Company

☐ Other (please identify): \_\_\_\_\_

B. Please indicate your level of satisfaction with each section of this issue of *The SAR Activity Review- Trends Tips and Issues* (circle your response).

1=Not Useful, 5=Very Useful

Section 1 - Director's Forum	1	2	3	4	5
Section 2 - Trends and Analysis	1	2	3	4	5
Section 3 - Law Enforcement Cases	1	2	3	4	5
Section 4 - Issues & Guidance	1	2	3	4	5
Section 5 - Industry Forum	1	2	3	4	5
Section 6 - Feedback Form	1	2	3	4	5

*Financial Crimes Enforcement Network*

C. What information or article in this edition did you find the most helpful or interesting? Please explain why (please indicate by topic title and page number):

---

---

---

D. What information did you find least helpful or interesting? Please explain why (again, please indicate by topic title and page number):

---

---

---

E. What new TOPICS, TRENDS, or PATTERNS in suspicious activity would you like to see addressed in the next edition of *The SAR Activity Review – Trends, Tips & Issues*? Please be specific - Examples might include: in a particular geographic area; concerning a certain type of transaction or instrument; other hot topics, etc.

---

---

---

F. What questions does your financial institution have about *The SAR Activity Review* that need to be answered?

---

---

---

G. Which of the previous issues have you read? (Check all that apply)

- |  |  |
|--|--|
| <input type="checkbox"/> Issue 1 - October 2000  | <input type="checkbox"/> Issue 2 - June 2001     |
| <input type="checkbox"/> Issue 3 - October 2001  | <input type="checkbox"/> Issue 4 - August 2002   |
| <input type="checkbox"/> Issue 5 - February 2003 | <input type="checkbox"/> Issue 6 - November 2003 |
| <input type="checkbox"/> Issue 7 - August 2004   | <input type="checkbox"/> Issue 8 - April 2005    |
| <input type="checkbox"/> Issue 9 - October 2005  | <input type="checkbox"/> Issue 10 - May 2006     |
| <input type="checkbox"/> Issue 11 - May 2007     | <input type="checkbox"/> Issue 11 - October 2007 |
| <input type="checkbox"/> Issue 13 - May 2008     | <input type="checkbox"/> Issue 14 - October 2008 |

*Financial Crimes Enforcement Network*

The *SAR Activity Review* **Index** is now available on the FinCEN website at:

[http://www.fincen.gov/news\\_room/rp/files/reg\\_sar\\_index.html](http://www.fincen.gov/news_room/rp/files/reg_sar_index.html)

For your convenience, topics are indexed alphabetically by subject matter.

The **Archive of Law Enforcement Cases** published in *The SAR Activity Review* can be accessed through the following link:

[http://www.fincen.gov/news\\_room/rp/sar\\_case\\_example.html](http://www.fincen.gov/news_room/rp/sar_case_example.html)



